

PSEUDOPRIMES STRONGER THAN STRONG PSEUDOPRIMES

JOHN H. CASTILLO, GILBERTO GARCÍA-PULGARÍN,
AND JUAN MIGUEL VELÁSQUEZ-SOTO

ABSTRACT. We introduce a new class of pseudoprimes. In this work we characterize Midy pseudoprimes, give some of their properties and established interesting connections with other known pseudoprimes, in particular we show that every divisor of a Midy pseudoprime is either a prime or a Midy pseudoprime and in the last case it is a strong pseudoprime.

1. MIDY'S PROPERTY

Let b be a positive integer greater than 1, b will denote the base of numeration, N a positive integer relatively prime to b , i.e $(N, b) = 1$, $|b|_N$ the order of b in the multiplicative group \mathbb{U}_N of positive integers less than N and relatively primes to N , and $x \in \mathbb{U}_N$. It is well known that when we write the fraction $\frac{x}{N}$ in base b , it is periodic. By period we mean the smallest repeating sequence of digits in base b in such expansion, it is easy to see that $|b|_N$ is the length of the period of the fractions $\frac{x}{N}$ (see Exercise 2.5.9 in [Nat00]). Let d, k be positive integers with $|b|_N = dk$, $d > 1$ and $\frac{x}{N} = 0.\overline{a_1 a_2 \cdots a_{|b|_N}}$ where the bar indicate the period and a_i 's are digits in base b . We separate the period $a_1 a_2 \cdots a_{|b|_N}$ in d blocks of length k and let

$$A_j = [a_{(j-1)k+1} a_{(j-1)k+2} \cdots a_{jk}]_b$$

be the number represented in base b by the j -th block and $S_d(x) = \sum_{j=1}^d A_j$.

If for all $x \in \mathbb{U}_N$, the sum $S_d(x)$ is a multiple of $b^k - 1$ we say that N has the Midy's property for b and d . It is named after E. Midy (1836), to read historical aspects about this property see [Lew07] and its references.

We denote with $\mathcal{M}_b(N)$ the set of positive integers d such that N has the Midy's property for b and d and we will call it the Midy's set of N to base b . As usual, let $\nu_p(N)$ be the greatest exponent of p in the prime factorization of N .

For example 13 has the Midy's property to the base 10 and $d = 3$, because $|13|_{10} = 6$, $1/13 = 0.\overline{076923}$ and $07 + 69 + 23 = 99$. Also, 75 has the Midy's property to the base 8 and $d = 4$, since $|75|_8 = 20$, $1/75 = [0.\overline{00664720155164033235}]_8$ and $[00664]_8 + [72015]_8 + [51640]_8 + [33235]_8 =$

$2 * (8^5 - 1)$. But 75 does not have the Midy's property to 8 and 5. Actually, we can see that $\mathcal{M}_{10}(13) = \{2, 3, 6\}$ and $\mathcal{M}_8(75) = \{4, 20\}$.

In [GPG09] is given the following characterization of Midy's property.

Theorem 1. *If N is a positive integer and $|b|_N = kd$, then $d \in \mathcal{M}_b(N)$ if and only if $\nu_p(N) \leq \nu_p(d)$ for all prime divisor p of $(b^k - 1, N)$.*

The next theorem is a different way to write Theorem 1.

Theorem 2. *Let N be a positive integer and d a divisor of $|b|_N$. The following statements are equivalent*

- (1) $d \in \mathcal{M}_b(N)$
- (2) *For each prime divisor p of N such that $\nu_p(N) > \nu_p(d)$, there exists a prime q divisor of $|b|_N$ that satisfies $\nu_q(|b|_p) > \nu_q(|b|_N) - \nu_q(d)$.*

In [CGPVS11] the authors prove the following theorem.

Theorem 3. *Let d_1, d_2 be divisors of $|b|_N$ and assume that $d_1 \mid d_2$ and $d_1 \in \mathcal{M}_b(N)$, then $d_2 \in \mathcal{M}_b(N)$.*

It is easy to see that if N is a prime number, then any divisor of $|b|_N$ greater than 1 is an element of $\mathcal{M}_b(N)$. In the next section, we will study when a given composite number N satisfies the above property. To do that and by the last theorem it is important to know when a prime divisor of $|b|_N$ is in $\mathcal{M}_b(N)$. It was characterized by the authors in [CGPVS12, Corollary 5]. We recall that result here.

Theorem 4 ([CGPVS12], Corollary 5). *Let N be a positive integer and let q be a prime divisor of $|b|_N$, then $q \in \mathcal{M}_b(N)$ if and only if*

- (1) *If $(N, q) = 1$, then $\nu_q(|b|_p) = \nu_q(|b|_N)$ for all p prime divisor of N .*
- (2) *If $(N, q) > 1$, then q^2 not divides N and $\nu_q(|b|_p) = \nu_q(|b|_N)$ for all p prime divisor of N different from q .*

2. MIDY PSEUDOPRIMES

Pomerance and Crandall in their book [CP05], state that:

Suppose we have a theorem, “If n is prime, then S is true about n ,” where “ S ” is some easily checkable arithmetic statement. If we are presented with a large number n , and we wish to decide whether n is prime or composite, we may very well try out the arithmetic statement S and see whether it actually holds for n . If the statement fails, we have proved the theorem that n is composite. If the statement holds, however, it may be that n is prime, and it also may be that n is composite. So we have the notion of S -pseudoprime, which is a composite integer for which S holds.

Applying the above commentary, to the Fermat's little theorem the concepts of pseudoprime and strong pseudoprime are given as follows

Definition 5. *The composite integer N is called a pseudoprime (or Fermat pseudoprime) to base b if $(b, N) = 1$ and $b^{N-1} \equiv 1 \pmod{N}$. An integer which is pseudoprime for all possible bases b is called a Carmichael number or an absolute pseudoprime. An odd composite N such that $N - 1 = 2^r s$ with s an odd integer and $(b, N) = 1$, is said to be a strong pseudoprime to base b if either $b^s \equiv 1 \pmod{N}$ or $b^{2^i s} \equiv -1 \pmod{N}$, for some $0 < i < r$.*

Proposition 6. *An odd composite integer N is a strong pseudoprime to base b if and only if N is pseudoprime to base b and there is a non-negative integer k such that $\nu_2(|b|_{p^{\nu_p(N)}}) = \nu_2(|b|_p) = k$ for all prime p divisor of N .*

Proof. Let $N - 1 = 2^t s$. Assume that N is pseudoprime to base b and $\nu_2(|b|_{p^{\nu_p(N)}}) = k$, for some non-negative integer k and for any prime divisor p of N . If $k = 0$, it follows that $|b|_N$ is odd and as $b^{N-1} \equiv 1 \pmod{N}$, then $b^s \equiv 1 \pmod{N}$. If $k > 0$, let $|b|_{p^{\nu_p(N)}} = 2^k s_p$, then $b^{2^{k-1} s_p} \equiv -1 \pmod{p^{\nu_p(N)}}$ and thus $b^{2^{k-1} s} \equiv -1 \pmod{N}$ for each prime divisor p of N . Therefore, in any case we obtain that N is a strong pseudoprime to base b . The reciprocal can be prove in a similar way. \square

The smallest absolute pseudoprime is 561 and in general such numbers are square-free and product of at least three primes, Alford et al. in [AGP94] proved that there are infinitely many absolute pseudoprimes.

Theorem 1 implies that if N is prime then N verifies the Midy's property for any base b and for all divisor d , different from 1, of $|b|_N$, this fact and the commentary quoted from Pomerance and Crandall leave us to study "Midy pseudoprimes" and we will dedicate the rest of this work to do it.

Theorem 7. *If N is a positive integer such that for all $d > 1$ and divisor of $|b|_N$ is satisfied that $d \in \mathcal{M}_b(N)$, then $(N, |b|_N)$ is either 1 or a prime.*

Proof. Let $p_1 < p_2$ be prime divisors of $(N, |b|_N)$. Write $N = p_1 p_2 N_1$ for some integer N_1 , therefore $|b|_N = p_1 p_2 [|b|_{p_1}, |b|_{p_2}] r$; with r an integer. Let $d = p_2$, $|b|_N = p_2 k$, because $|b|_{p_1}$ divides k it follows that $p_1 \mid (N, b^k - 1)$ and since $d \in \mathcal{M}_b(N)$ we have $\nu_{p_1}(N) \leq \nu_{p_1}(d)$, which is a contradiction as $1 < \nu_{p_1}(N)$ and $\nu_{p_1}(d) = \nu_{p_1}(p_2) = 0$. It is clear that p^2 not divides $(N, |b|_N)$. \square

Theorem 8. *Let N be a positive integer, then $d \in \mathcal{M}_b(N)$ for all divisor $d > 1$ of $|b|_N$, if and only if*

- (1) *If $(N, |b|_N) = 1$, then $N = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ with each p_i prime and $|b|_N = |b|_{p_i}$ for $i = 1, \dots, l$.*
- (2) *If $(N, |b|_N) = r$ prime, then $N = r p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ with each p_i prime and $|b|_N = |b|_{p_i} = r^s |b|_r$ for $i = 1, \dots, l$ with s a positive integer.*

Proof. From Theorem 3, it is clear that $d \in \mathcal{M}_b(N)$ for all divisor $d > 1$ of $|b|_N$ if and only if $q \in \mathcal{M}_b(N)$ for each prime divisor q of $|b|_N$. The part (1) is immediate from the first case of Theorem 4.

To prove the second part, assume that $d \in \mathcal{M}_b(N)$ for all divisor $d > 1$ of $|b|_N$. From Theorem 7 we have $r = (N, |b|_N)$ for some prime r . Take $N = rN_1$ with N_1 an integer and $|b|_N = r^s |b|_r h$ where $(h, r) = 1$. We will prove that $h = 1$. If there is a prime divisor q of h , from Theorem 4 follows that $\nu_q(|b|_N) = \nu_q(|b|_p)$ for all prime divisor p of N , particularly to $p = r$ we obtain $\nu_q(|b|_r) = \nu_q(|b|_N) = \nu_q(|b|_r) + \nu_q(h)$ and hence $\nu_q(h) = 0$. Thus $h = 1$.

Let $p \neq r$ a prime which divides N , we will see that $|b|_N = |b|_p$. Write $|b|_N = |b|_p H$ with H an integer. If p is a divisor of H , then p divides $|b|_N$ and consequently p divides $(N, |b|_N)$ which is absurd because $p \neq r$. Suppose that there exists a prime q different from p and divisor of H , so $|b|_N = |b|_p H = |b|_p H_1 q = qk$ and as, by the assumption, $q \in \mathcal{M}_b(N)$, it leaves us to a contradiction from Theorem 1 because p is a divisor of $(N, b^k - 1)$. So $H = 1$ and $|b|_p = |b|_N = r^s |b|_r$. Therefore $N = rp_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$ with each p_i prime and also $|b|_N = |b|_{p_i} = r^s |b|_r$.

Conversely, assume that $N = rp_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$, $(N, |b|_N) = r$ and $|b|_N = |b|_{p_i} = r^s |b|_r$. Take $d > 1$ a divisor of $|b|_N$, $|b|_N = kd$ and let $g = (N, b^k - 1)$. Since $|b|_{p_i} = |b|_N = kd$ for each $1 \leq i \leq l$, we obtain that $|b|_{p_i}$ is not a divisor of k therefore p_i does not divide g . Thus either $g = 1$ or $g = r$. In any case, by Theorem 1, N has the Midy's property for b and d . \square

Definition 9. We say that a number N is a Midy pseudoprime to base b if N is an odd composite number relatively prime to both b and $|b|_N$ and for all divisor $d > 1$ of $|b|_N$ we get that $d \in \mathcal{M}_b(N)$.

By this definition the first part of Theorem 8 can be write in the following way.

Theorem 10. An odd composite number $N = p_1^{e_1} p_2^{e_2} \cdots p_l^{e_l}$, with p_i 's different primes and N relatively prime to b , is a Midy pseudoprime to base b if and only if $|b|_N = |b|_{p_i}$ for every $1 \leq i \leq l$.

V. Shevelev defines in [She08] the concept of overpseudoprime numbers and characterized them in Theorem 7. That result is equivalent to our Theorem 10, so the concepts of overpseudoprime and Midy's pseudoprime agree.

Theorem 10 give us the following characterization.

Corollary 11. An odd composite N is a Midy pseudoprime to base b if and only if each divisor of N is either a prime or a Midy pseudoprime to base b .

The bellow result, Theorem 2.3 of [Mot95], allows us to give a equivalent form of Theorem 10. We denote with $\Phi_n(x)$ the n -th cyclotomic polynomial.

Theorem 12 (Theorem 2.3 of [Mot95]). *Let $m, b \geq 2, n \geq 3$ and p be integers, where p is the greatest prime divisor of n . Then a composite number m is a divisor of $\Phi_n(b)$ if and only if $b^n \equiv 1 \pmod{m}$ and every prime divisor q of m satisfies that*

$$n = \begin{cases} |b|_q & \text{if } q \neq p, \\ p^e |b|_p & \text{if } q = p. \end{cases}$$

The following result is a consequence of Theorems 10 and 12.

Theorem 13. *A composite number N with $(N, |b|_N) = 1$, is a Midy pseudoprime to base b if and only if $\Phi_{|b|_N}(b) \equiv 0 \pmod{N}$ and $|b|_N > 1$.*

Theorem 1 of [PSW80] shows the subsequent result for strong pseudoprimes. We present here a more wide version which is a direct consequence of Theorems 10 and 12.

Theorem 14. *Let $N > 2$ and $f_N(b) = \frac{\Phi_N(b)}{(N, \Phi_N(b))}$. If $f_N(b)$ is composite, then $f_N(b)$ is a Midy pseudoprime to base b .*

Our next result extends Theorem 3.5.10 of [CP05].

Theorem 15. *Let p be an odd prime and $1 < b < p - 1$, then $N = \frac{b^p + 1}{b + 1}$ is either a Midy pseudoprime to base b or a prime.*

Proof. It is well known that n odd implies that $\Phi_{2n}(b) = \Phi_n(-b)$ and from here $N = \frac{b^p + 1}{b + 1} = \Phi_p(-b) = \Phi_{2p}(b)$. In consequence, N is odd and congruent with 1 mod p . Therefore, $(2p, \Phi_{2p}(b)) = 1$ and the result follows from the last theorem. \square

The set of bases of Midy pseudoprimality is closed respect to powers, although it is not closed by product as we can see when take $N = 91$ which is Midy pseudoprime to bases 9 and 16 but it is not to 53, their product modulo N .

Theorem 16. *If N is a Midy pseudoprime to base b , then N is Midy pseudoprime to base b^t for any positive integer $t \geq 1$.*

Proof. The result is immediate from Theorem 10, since N is Midy pseudoprime to base b so $|b|_N = |b|_p$ for each prime divisor p of N . Now $|b^t|_N = \frac{|b|_N}{(t, |b|_N)} = \frac{|b|_p}{(t, |b|_p)} = |b^t|_p$. It shows that N is a Midy pseudoprime to base b^t . \square

Theorem 17. *If N is a Midy pseudoprime to base b , then N is a pseudoprime to base b .*

Proof. Write $N = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$ and assume that N is a Midy pseudoprime to base b . From Theorem 10 follows $|b|_N = |b|_{p_i} = |b|_{p_i^{e_i}} = t$ for each $i = 1, 2, \dots, l$. By the assumption we get that $t \mid p_i - 1$ for each $i = 1, 2, \dots, l$

and thus $b^{p_j-1} \equiv 1 \pmod{p_i^{e_i}}$ for all pair i, j . So, $b^{p_j} \equiv b \pmod{p_i^{e_i}}$ and from here $b^{p_j^{e_j}} \equiv b \pmod{p_i^{e_i}}$ and, consequently, $b^{p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}} \equiv b \pmod{p_i^{e_i}}$, namely $b^N \equiv b \pmod{p_i^{e_i}}$ for each i and therefore $b^N \equiv b \pmod{N}$. \square

Theorem 18. *If N is a Midy pseudoprime to base b , then N is a strong pseudoprime to base b .*

Proof. Write $N = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$ and assume that N is a Midy pseudoprime to base b . We know that N is a pseudoprime to base b . Since N is a Midy pseudoprime to base b implies that $|b|_N = |b|_n$ for each divisor n of N and thus there is a non-negative integer k such that for all prime divisor p of N we get that $\nu_2(|b|_{p^{\nu_p(N)}}) = k$ and the result follows from Proposition 6. \square

The reciprocal is not true. For example $N = 91$ is a strong pseudoprime to base 53, but this is not a Midy pseudoprime to this base.

Additionally, from the last theorem and Corollary 11 we get that every composite divisor of a Midy pseudoprime is a strong pseudoprime, in this sense the Midy pseudoprimes are stronger than strong pseudoprimes.

Among the first 58892 strong pseudoprimes to base 2 there are only 31520 Midy pseudoprimes to base 2. Similarly, to base 3 there are 2558 Midy pseudoprimes in the first 6087 strong pseudoprimes and we found 582 Midy pseudoprimes to base 5 in the first 1288 strong pseudoprime to base 5. Almost the 47% of the strong pseudoprimes are Midy pseudoprimes.

We denote with ψ_k and $\tilde{\psi}_k$ the smallest strong pseudoprime and the smallest Midy pseudoprime to all the first k primes taken as bases, respectively. From Theorem 18 we know that $\psi_k \leq \tilde{\psi}_k$ for every positive integer k . With some calculations, we can see that $\psi_1 = 2047$, $\tilde{\psi}_2 = 5173601$ and $\tilde{\psi}_3 = 960946321$. We know, by [Jae93], the exact values for ψ_k , with $1 \leq k \leq 8$. Thus, $\tilde{\psi}_4 > 3215031751 = \psi_4$, $\tilde{\psi}_5 > 2152302898747 = \psi_5$, $\tilde{\psi}_6 > 3474749660383 = \psi_6$, $\tilde{\psi}_7 > 341550071728321 = \psi_7$ and $\tilde{\psi}_8 > 341550071728321 = \psi_8$.

ACKNOWLEDGEMENTS

The authors are members of the research group: Álgebra, Teoría de Números y Aplicaciones, ERM. J.H. Castillo was partially supported by CAPES, CNPq from Brazil and Universidad de Nariño from Colombia. J.M. Velásquez-Soto was partially supported by CONICET from Argentina and Universidad del Valle from Colombia.

REFERENCES

- [AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR 1283874 (95k:11114)

- [CGPVS11] John H. Castillo, Gilberto García-Pulgarín, and Juan Miguel Velásquez-Soto, *Structure of associated sets to Midy's Property*, accepted to publication in *Matemáticas: Enseñanza Universitaria*, arXiv:1110.3308v2 [math.NT] (2011).
- [CGPVS12] ———, *On a particular case of the Dirichlet's theorem and Midy's property*, arXiv:1203.1273v1 [math.NT] (2012).
- [CP05] Richard Crandall and Carl Pomerance, *Prime numbers*, second ed., Springer, New York, 2005, A computational perspective. MR 2156291 (2006a:11005)
- [GPG09] Gilberto García-Pulgarín and Hernán Giraldo, *Characterizations of Midy's property*, *Integers* **9** (2009), A18, 191–197. MR MR2506150
- [Jae93] Gerhard Jaeschke, *On strong pseudoprimes to several bases*, *Math. Comp.* **61** (1993), no. 204, 915–926. MR 1192971 (94d:11004)
- [Lew07] Joseph Lewittes, *Midy's theorem for periodic decimals*, *Integers* **7** (2007), A2, 11 pp. (electronic). MR MR2282184 (2008c:11004)
- [Mot95] Kaoru Motose, *On values of cyclotomic polynomials. II*, *Math. J. Okayama Univ.* **37** (1995), 27–36 (1996). MR 1416242 (97h:11151)
- [Nat00] Melvyn B. Nathanson, *Elementary methods in number theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000. MR 1732941 (2001j:11001)
- [PSW80] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff, Jr., *The pseudo-primes to $25 \cdot 10^9$* , *Math. Comp.* **35** (1980), no. 151, 1003–1026. MR 572872 (82g:10030)
- [She08] V. Shevelev, *Overpseudoprimes, Mersenne Numbers and Wieferich primes*, arXiv:0806.3412v7 [math.NT] (2008).

JOHN H. CASTILLO, DEPARTAMENTO DE MATEMÁTICAS Y ESTADÍSTICA, UNIVERSIDAD DE NARIÑO, SAN JUAN DE PASTO-COLOMBIA
E-mail address: jhcastillo@gmail.com

GILBERTO GARCÍA-PULGARÍN, UNIVERSIDAD DE ANTIOQUIA, MEDELLÍN-COLOMBIA
E-mail address: gigarcia@ciencias.udea.edu.co

JUAN MIGUEL VELÁSQUEZ-SOTO, DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL VALLE, CALI-COLOMBIA
E-mail address: jumiveso@univalle.edu.co